**TOFEDU: The Future of Education Journal**
Volume 4 Number 4 (2025) Page: 821-829
E-ISSN 2961-7553 P-ISSN 2963-8135
https://journal.tofedu.or.id/index.php/journal/index

# A Literature Review on The Transformation of Defense Law in The Digital Age and Advanced Technology

## KAJIAN LITERATUR TENTANG TRANSFORMASI HUKUM PERTAHANAN DI ERA DIGITAL DAN TEKNOLOGI CANGGIH

**Ahmad Jaeni[1], Sinthu Bas Ignatius[2], Ateng Karsoma[3]**
jaeni2199@gmail.com, sinthubasignatius@gmail.com, akarsomasthm@gmail.com
Magister Hukum Militer, Sekolah Tinggi Hukum Militer (AHM-PTHM), Kota Jakarta Timur

## ABSTRACT
This study aims to examine the transformation of defense law in the digital age and advanced technology, focusing on the impact of technological advancements on national defense policies and regulations. With the rapid development of technology, particularly cyber threats that cross territorial boundaries, national defense legal systems face new challenges that require updates to regulations and policies. Through a literature review, this research identifies that traditional defense law needs to be revised to include protection of critical infrastructure, regulation of technology-based defense, and management of digital threats. Advanced technologies such as artificial intelligence, big data, and the Internet of Things provide opportunities to strengthen defense systems, but they also pose ethical and legal challenges, particularly regarding privacy, human rights, and accountability in the use of technology in military operations. The study also emphasizes the importance of international collaboration in addressing global transnational cyber threats. As a recommendation, countries need to urgently update their defense law regulations and strengthen international cooperation to maintain global security, while ensuring the use of defense technology aligns with international law principles and human rights.

**Keywords: defense law, digital transformation, cyber threats, technology.**

## PENDAHULUAN
Perkembangan pesat dalam teknologi digital dan canggih telah membawa dampak signifikan pada berbagai sektor kehidupan, termasuk bidang hukum (Hakim & Yulia, 2024). Salah satu aspek yang terkena dampak adalah hukum pertahanan, yang menjadi sangat penting di era modern ini untuk menjaga kedaulatan dan keamanan negara (Budi et al., 2021). Seiring dengan munculnya berbagai inovasi dalam teknologi informasi, perang siber, dan ancaman-ancaman baru yang memanfaatkan kemajuan teknologi, hukum pertahanan perlu mengalami transformasi agar dapat mengakomodasi tantangan tersebut. Seperti yang diungkapkan oleh Aris & Lelyana, (2023), hukum pertahanan harus mampu beradaptasi dengan cepat terhadap perkembangan teknologi untuk memastikan keberlanjutan sistem pertahanan yang efektif di era digital.





E-ISSN 2961-7553
P-ISSN 2963-8135

Kajian literatur tentang transformasi hukum pertahanan di era digital dan teknologi canggih ini bertujuan untuk menggali pemahaman tentang bagaimana perubahan teknologi memengaruhi sistem hukum pertahanan suatu negara. Sebagai contoh, keberadaan kecerdasan buatan (AI), big data, dan internet of things (IoT) telah mengubah cara pandang negara terhadap ancaman, baik yang datang dari dalam maupun luar negeri. Menurut Keliat, (2024), teknologi digital telah menciptakan tantangan baru yang mengharuskan negara untuk memperbarui kerangka hukum mereka guna menjaga stabilitas dan keamanan negara.

Hukum pertahanan, yang pada masa sebelumnya cenderung fokus pada aspek fisik dan tradisional, kini harus menghadapi ancaman yang lebih terdistribusi dan berbasis teknologi. Hal ini terutama terlihat dalam dinamika ancaman siber, yang memerlukan pendekatan baru dalam hukum pertahanan untuk mencegah dan menangani serangan yang bisa merusak infrastruktur kritis dan data sensitif. Hal ini diakui oleh Ichsan, (2024) yang menyatakan bahwa, ancaman siber yang semakin kompleks menuntut adanya peran hukum yang lebih besar dalam menjaga keamanan dunia maya, serta pembaruan pada kebijakan pertahanan yang berbasis teknologi. Dalam konteks ini, transformasi hukum pertahanan bukan hanya berkaitan dengan perubahan regulasi atau norma yang ada, tetapi juga dengan bagaimana negara merespons secara cepat terhadap berbagai ancaman yang muncul akibat kemajuan teknologi. Seperti yang dikemukakan oleh (Savitri, 2024), hukum pertahanan di era digital harus lebih fleksibel dan dinamis untuk merespons ancaman yang selalu berubah. Dengan demikian, diperlukan kajian yang lebih dalam untuk melihat bagaimana negara dapat memperkuat sistem pertahanan mereka melalui kebijakan hukum yang tepat.

Melalui kajian literatur ini, diharapkan dapat ditemukan pemahaman yang lebih baik tentang perlunya pembaruan dan penyempurnaan dalam regulasi hukum pertahanan, serta bagaimana negara-negara dapat memanfaatkan kemajuan teknologi digital dengan tetap menjaga prinsip-prinsip hukum internasional dan keamanan nasional. Sebagai upaya untuk mengantisipasi perkembangan ancaman yang semakin kompleks, transformasi hukum pertahanan menjadi sebuah keniscayaan yang tidak bisa dihindari. Di masa depan, hukum pertahanan harus melibatkan lebih banyak elemen teknologi untuk memberikan perlindungan yang lebih kuat dan holistik (Syafi'i et al., 2023).

Kajian ini diharapkan dapat memberi sumbangan pemikiran terhadap bagaimana mengintegrasikan aspek teknologi dalam kebijakan hukum pertahanan secara komprehensif. Hal ini penting agar negara-negara dapat menjaga kedaulatan dan keamanannya dengan efektif, sekaligus memanfaatkan potensi teknologi untuk memperkuat sistem pertahanan mereka. Seperti yang ditekankan oleh Sarjito, (2024) transformasi hukum pertahanan yang berbasis teknologi canggih merupakan langkah penting untuk memastikan bahwa pertahanan negara tetap relevan di tengah dinamika ancaman global yang terus berkembang. Dengan demikian, kajian literatur ini bertujuan untuk mengidentifikasi dan menganalisis berbagai perubahan yang terjadi dalam hukum pertahanan akibat perkembangan teknologi digital dan canggih, serta memberikan rekomendasi untuk adaptasi yang lebih baik di masa depan.

## METODE

Penelitian ini menggunakan pendekatan kajian literatur atau studi pustaka yang bersifat deskriptif-analitis. Metode ini dipilih untuk menggali, menganalisis, dan menginterpretasikan berbagai sumber yang relevan terkait dengan transformasi hukum pertahanan di era digital dan teknologi canggih. Penelitian ini bertujuan untuk mengidentifikasi tren, pola, dan perubahan dalam konsep serta implementasi hukum pertahanan akibat pengaruh teknologi modern.



E-ISSN 2961-7553
P-ISSN 2963-8135

1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan mengutamakan analisis mendalam terhadap berbagai literatur yang berkaitan dengan topik utama, yaitu hukum pertahanan dan teknologi canggih. Pendekatan kualitatif memungkinkan peneliti untuk mendapatkan pemahaman yang lebih komprehensif mengenai bagaimana perkembangan teknologi berdampak pada hukum pertahanan dan apa saja tantangan yang dihadapi oleh negara dalam menyesuaikan regulasi pertahanan di era digital.

2. Sumber Data

Data yang digunakan dalam penelitian ini bersumber dari berbagai literatur yang relevan, seperti buku, artikel jurnal ilmiah, laporan penelitian, dokumen kebijakan, serta sumber-sumber lain yang membahas topik hukum pertahanan dan teknologi canggih. Proses pencarian literatur dilakukan melalui database akademik, seperti Google Scholar, JSTOR, ScienceDirect, dan ProQuest, yang menyediakan artikel-artikel ilmiah terkini terkait dengan topik penelitian ini.

3. Kriteria Pemilihan Sumber

Sumber literatur yang digunakan dalam penelitian ini dipilih berdasarkan relevansi dan kredibilitasnya. Kriteria pemilihan sumber meliputi:

a. Literatur yang diterbitkan dalam 10 tahun terakhir untuk memastikan bahwa informasi yang diperoleh mencerminkan perkembangan terbaru dalam hukum pertahanan dan teknologi.
b. Artikel atau buku yang diterbitkan oleh ahli di bidang hukum pertahanan, teknologi, dan kebijakan internasional.
c. Dokumen kebijakan dan regulasi yang diterbitkan oleh pemerintah atau organisasi internasional yang mengatur aspek hukum pertahanan dan ancaman siber.

## HASIL DAN PEMBAHASAN

Dalam bagian ini, hasil penelitian yang diperoleh dari kajian literatur akan disajikan dan dianalisis secara mendalam. Penelitian ini bertujuan untuk mengidentifikasi transformasi hukum pertahanan di era digital dan teknologi canggih. Berdasarkan analisis terhadap berbagai literatur yang relevan, ditemukan sejumlah temuan utama yang berkaitan dengan pengaruh teknologi terhadap hukum pertahanan, tantangan yang dihadapi negara, serta langkah-langkah yang diambil dalam menanggapi perubahan tersebut.

### Transformasi Hukum Pertahanan akibat Teknologi Canggih

Hukum pertahanan mengalami perubahan signifikan seiring dengan pesatnya perkembangan teknologi. Sebelumnya, hukum pertahanan lebih fokus pada aspek fisik dan konvensional, seperti penggunaan angkatan bersenjata untuk melindungi kedaulatan negara (Sa'diyah & Vinata, 2016). Perlindungan ini umumnya berbentuk upaya pertahanan terhadap ancaman militer yang nyata, seperti invasi atau serangan langsung dari negara lain. Namun, dengan kemajuan teknologi, ancaman terhadap negara semakin beragam dan kompleks, khususnya yang bersifat non-fisik.

Ancaman yang muncul di era digital, seperti serangan siber dan manipulasi informasi, telah memaksa hukum pertahanan untuk beradaptasi (Duarte, 2024). Serangan siber tidak hanya mengancam keamanan dunia maya, tetapi juga infrastruktur kritis yang dapat memengaruhi stabilitas negara. Manipulasi informasi, yang seringkali dilakukan melalui media sosial atau platform digital lainnya, juga dapat merusak kepercayaan publik dan mempengaruhi kestabilan politik. Oleh karena itu, hukum pertahanan harus memperluas cakupannya untuk melindungi negara dari ancaman-ancaman berbasis digital ini. Hukum pertahanan kini harus mencakup regulasi yang mengatur perlindungan dunia maya dan infrastruktur kritis (Irvita et al., 2025). Dalam konteks ini, negara tidak hanya perlu



E-ISSN 2961-7553
P-ISSN 2963-8135

mempertahankan diri melalui kekuatan militer, tetapi juga dengan kebijakan yang dapat melindungi sistem teknologi dan data penting. Ancaman dari dunia maya, yang tidak mengenal batas teritorial, memerlukan pendekatan yang lebih luas dan fleksibel dalam hal peraturan dan kebijakan yang ada.

Di sisi lain, kebijakan yang ada perlu diperbarui untuk dapat merespons ancaman dunia maya dengan cepat dan efektif. Dalam menghadapi serangan siber, respons yang lambat atau kurang terkoordinasi dapat berisiko tinggi, mengingat dampaknya yang dapat menyebar dengan sangat cepat dan luas. Oleh karena itu, penting bagi negara untuk memiliki regulasi yang memungkinkan kerjasama lintas batas dengan negara lain, serta kemampuan untuk melibatkan sektor swasta dalam perlindungan infrastruktur kritis.

Secara keseluruhan, transformasi dalam hukum pertahanan ini mencerminkan perubahan paradigma dalam menjaga keamanan negara. Ke depannya, hukum pertahanan tidak hanya akan mencakup perlindungan fisik melalui angkatan bersenjata, tetapi juga harus mencakup strategi digital dan regulasi yang lebih komprehensif. Negara harus siap untuk menghadapi ancaman siber yang semakin canggih dan bersifat transnasional dengan pendekatan hukum yang lebih inklusif dan dinamis.

**Ancaman Siber dan Peran Hukum Pertahanan**

Ancaman siber kini menjadi salah satu tantangan terbesar yang dihadapi oleh sistem pertahanan modern. Menurut Kurniati, (2024), serangan siber memiliki potensi untuk mengancam infrastruktur vital negara, seperti jaringan energi, sistem transportasi, dan data sensitif yang berkaitan dengan keamanan nasional. Ancaman ini sangat berbahaya karena dapat merusak sistem yang mengendalikan berbagai sektor kehidupan masyarakat, dari pemerintahan hingga sektor swasta, yang sangat bergantung pada teknologi informasi. Oleh karena itu, hukum pertahanan harus beradaptasi dengan cepat untuk mengatasi dan merespons ancaman siber ini.

Perubahan yang diperlukan dalam hukum pertahanan adalah penguatan regulasi terkait keamanan siber serta pembentukan kebijakan pertahanan yang lebih dinamis dan responsif terhadap ancaman digital. Sistem pertahanan tradisional yang mengutamakan aspek fisik dan militer kini perlu melibatkan kebijakan yang lebih luas dan komprehensif, mencakup perlindungan terhadap dunia maya. Dalam menghadapi ancaman siber yang terus berkembang, peraturan yang ada harus lebih fleksibel agar dapat mengantisipasi jenis serangan yang semakin canggih dan kompleks.

Beberapa negara telah mulai mengintegrasikan aspek siber dalam hukum pertahanan mereka untuk menghadapi tantangan ini. Amerika Serikat, misalnya, telah mengembangkan *"Cyber Command,"* sebuah unit yang bertanggung jawab untuk melindungi sistem pertahanan siber negara. *Cyber Command* juga berfungsi untuk merespons ancaman siber secara lebih terkoordinasi dan efektif (Chotimah, 2020). Pembentukan badan khusus seperti ini menunjukkan keseriusan negara dalam menangani ancaman siber sebagai bagian dari strategi pertahanan nasional. Langkah-langkah ini menegaskan bahwa adaptasi hukum pertahanan terhadap ancaman siber bukan hanya penting, tetapi juga mendesak untuk dilakukan. Negara harus memiliki regulasi yang dapat menanggapi serangan siber dengan cepat dan terkoordinasi, karena dampak dari serangan semacam ini bisa sangat luas, melibatkan berbagai sektor dan berdampak langsung pada keamanan negara. Keamanan dunia maya bukan lagi hanya tugas lembaga teknologi, tetapi juga bagian dari kebijakan pertahanan negara secara keseluruhan.

Secara keseluruhan, ancaman siber memerlukan perubahan signifikan dalam pendekatan hukum pertahanan. Negara harus mampu melindungi infrastruktur digital yang menjadi tulang punggung sistem pertahanan mereka dan mengadaptasi regulasi untuk menghadapi ancaman yang tidak terduga. Dengan adanya kebijakan yang lebih dinamis dan



E-ISSN 2961-7553
P-ISSN 2963-8135

adaptif terhadap perkembangan teknologi, negara dapat meningkatkan ketahanan sistem pertahanan sibernya dan meminimalkan risiko dari ancaman siber yang semakin mengancam stabilitas nasional.

**3. Kebutuhan Pembaruan Regulasi Hukum Pertahanan**

Dalam merespons perkembangan teknologi yang pesat, banyak negara kini menyadari bahwa regulasi hukum pertahanan yang ada sudah tidak lagi memadai. Seperti yang dijelaskan oleh Chang (2023), negara-negara tidak dapat lagi mengandalkan regulasi lama yang tidak memperhitungkan ancaman yang timbul dari teknologi. Ancaman baru seperti serangan siber, manipulasi informasi, dan penyalahgunaan teknologi untuk tujuan destruktif semakin mendesak negara untuk memperbarui kerangka hukum pertahanannya. Pembaruan ini diperlukan untuk memastikan bahwa negara dapat menjaga kedaulatan dan keamanannya dengan lebih efektif di era digital.

Pembaruan hukum pertahanan ini mencakup beberapa aspek penting, seperti revisi terhadap undang-undang yang mengatur pertahanan negara, perlindungan data, serta respons terhadap serangan dunia maya. Regulasi yang lebih modern dan relevan akan memungkinkan negara untuk menangani ancaman-ancaman baru yang muncul dari perkembangan teknologi, yang sebelumnya tidak terduga. Hal ini penting agar negara tidak hanya mengandalkan pendekatan tradisional dalam pertahanan, tetapi juga mengintegrasikan elemen teknologi yang semakin dominan dalam berbagai sektor kehidupan.

Namun, tantangan besar yang dihadapi dalam proses pembaruan regulasi hukum pertahanan adalah adanya kesenjangan antara kecepatan perkembangan teknologi dan pembaruan regulasi yang seringkali berjalan lambat. Seiring dengan pesatnya inovasi di bidang teknologi, ancaman yang muncul juga semakin cepat dan kompleks, sementara regulasi yang ada seringkali tidak dapat mengikuti perkembangan tersebut. Kesenjangan ini menambah kesulitan bagi negara dalam merespons ancaman dengan cepat dan efektif, sehingga dapat mengurangi efektivitas sistem pertahanan yang ada.

Menurut Carter (2021), untuk mengatasi tantangan ini, negara perlu memiliki kebijakan yang lebih fleksibel dan proaktif dalam menyusun dan memperbarui regulasi hukum pertahanan. Kebijakan yang fleksibel ini akan memungkinkan negara untuk beradaptasi dengan cepat terhadap perubahan teknologi, serta memfasilitasi pembaruan yang lebih cepat. Kebijakan yang proaktif juga penting untuk mengantisipasi potensi ancaman yang belum muncul dan menyiapkan sistem pertahanan sejak dini, bukan hanya merespons setelah ancaman terjadi.

Secara keseluruhan, pembaruan regulasi hukum pertahanan merupakan langkah penting dalam menjaga keamanan dan kedaulatan negara di tengah perkembangan teknologi yang pesat. Negara harus mampu beradaptasi dengan cepat untuk mengatasi ancaman baru yang timbul dari dunia digital, melalui kebijakan dan regulasi yang lebih fleksibel, dinamis, dan responsif terhadap perubahan teknologi. Dengan pembaruan ini, diharapkan sistem pertahanan negara dapat tetap efektif dan relevan dalam menghadapi tantangan yang terus berkembang.

**Globalisasi Teknologi dan Dampaknya terhadap Hukum Pertahanan**

Globalisasi teknologi telah mengaburkan batas-batas teritorial negara, di mana ancaman digital kini dapat datang dari luar tanpa adanya kehadiran fisik. Salah satu contoh nyata dari fenomena ini adalah serangan siber yang dilakukan oleh negara atau aktor non-negara yang beroperasi di luar negeri (Kusuma, 2024). Serangan tersebut dapat menyebabkan kerusakan serius pada infrastruktur kritis suatu negara, seperti jaringan energi, sistem perbankan, atau layanan kesehatan, yang dapat mengganggu stabilitas nasional. Ancaman digital semacam ini memerlukan respon yang lebih global, mengingat dampaknya yang bisa melintasi batas-batas negara.



E-ISSN 2961-7553
P-ISSN 2963-8135

Untuk mengatasi ancaman ini, dibutuhkan adanya kolaborasi internasional dalam mengembangkan kebijakan hukum yang dapat mengatasi ancaman digital secara efektif. Sebagai contoh, serangan siber dari aktor asing sering kali sulit untuk diidentifikasi dan ditangani dengan cepat, terutama karena ancaman tersebut dapat datang dari lokasi yang jauh dan tidak terdeteksi dengan mudah oleh pertahanan nasional suatu negara. Oleh karena itu, negara-negara harus bekerja sama dalam merumuskan regulasi yang lebih global untuk menciptakan ketahanan yang lebih baik terhadap ancaman tersebut. Berlianti et al., (2024) mengemukakan bahwa ancaman yang bersifat transnasional, seperti serangan siber, memerlukan pendekatan hukum yang melibatkan kerja sama antara negara-negara. Hukum internasional perlu diperbarui agar dapat menangani ancaman yang tidak mengenal batas teritorial. Pembaruan ini akan memastikan bahwa negara-negara memiliki mekanisme yang lebih baik dalam merespons ancaman digital yang dapat mengganggu keamanan global. Tanpa adanya pengaturan yang jelas dan efektif, ancaman ini bisa semakin sulit untuk ditangani secara terpisah oleh masing-masing negara.

Kerja sama internasional dalam pengaturan hukum pertahanan berbasis teknologi menjadi salah satu langkah penting untuk memastikan keamanan bersama di tingkat internasional (Ardiyanti, 2014). Negara-negara harus berbagi informasi, berbagi teknologi, dan menyusun kebijakan bersama dalam menangani ancaman siber yang bersifat lintas negara. Dengan adanya kesepahaman dan kerangka kerja yang jelas, negara-negara dapat lebih efektif dalam mengatasi serangan siber dan memperkuat pertahanan mereka.

Secara keseluruhan, ancaman siber yang bersifat transnasional memerlukan pendekatan hukum yang lebih inklusif dan internasional. Kerja sama antarnegara dalam mengembangkan kebijakan hukum pertahanan berbasis teknologi adalah langkah yang penting untuk menjaga keamanan global. Negara-negara harus memperbarui hukum internasional dan membangun kolaborasi yang lebih erat dalam menghadapi ancaman siber, agar dapat menciptakan sistem pertahanan yang lebih tangguh dan responsif terhadap tantangan teknologi yang terus berkembang.

**Peran Teknologi dalam Modernisasi Sistem Pertahanan**

Teknologi canggih, selain menimbulkan ancaman baru, juga membuka peluang besar untuk memperkuat sistem pertahanan negara. Penggunaan kecerdasan buatan (AI), big data, dan *Internet of Things (IoT)* memungkinkan negara untuk meningkatkan kemampuan deteksi dan respons terhadap berbagai ancaman yang ada (Kristiyanti & Mahendro, 2025). Misalnya, AI dapat digunakan untuk memprediksi dan menganalisis ancaman siber dengan lebih cepat dan akurat, sementara big data memungkinkan analisis yang lebih mendalam terhadap pola serangan atau potensi ancaman yang mungkin terjadi, memberikan waktu yang lebih banyak bagi pihak berwenang untuk merespons.

Kemajuan teknologi ini, menurut Chatlina et al., (2024), dapat meningkatkan efektivitas operasional dan pengambilan keputusan dalam sistem pertahanan. Dengan bantuan teknologi, negara dapat mempercepat proses identifikasi dan mitigasi ancaman, serta meningkatkan kemampuan untuk melakukan analisis secara real-time. Hal ini tentu sangat penting dalam menghadapi ancaman yang semakin kompleks, yang sering kali muncul secara tiba-tiba dan membutuhkan respon yang cepat serta tepat. Namun, integrasi teknologi canggih ini juga membawa tantangan tersendiri. Penggunaan teknologi dalam sistem pertahanan, terutama yang melibatkan data sensitif dan analisis AI, memerlukan regulasi yang ketat untuk memastikan bahwa teknologi digunakan dengan cara yang sah. Tanpa regulasi yang tepat, ada risiko penyalahgunaan teknologi, seperti pelanggaran hak asasi manusia atau invasi terhadap privasi individu. Oleh karena itu, penting untuk menetapkan kerangka hukum yang jelas dan transparan dalam penggunaan teknologi dalam pertahanan.



E-ISSN 2961-7553
P-ISSN 2963-8135

Regulasi yang tepat juga menjadi kunci untuk memastikan bahwa teknologi tidak hanya digunakan untuk memperkuat pertahanan, tetapi juga untuk melindungi nilai-nilai dasar masyarakat, seperti kebebasan dan hak-hak privasi. Negara harus memastikan bahwa teknologi digunakan dengan cara yang bertanggung jawab, menjaga keseimbangan antara keamanan dan kebebasan individu. Oleh karena itu, pengembangan kebijakan dan hukum yang dapat mengatur penggunaan teknologi dalam pertahanan sangat penting.

Secara keseluruhan, teknologi canggih menawarkan potensi besar untuk memperkuat sistem pertahanan suatu negara. Dengan penggunaan AI, big data, dan IoT, negara dapat meningkatkan kemampuan deteksi, analisis, dan respons terhadap ancaman. Namun, untuk memanfaatkan potensi ini secara optimal, perlu adanya regulasi yang tepat yang mengatur penggunaan teknologi tersebut dengan cara yang sah, tidak melanggar hak asasi manusia, dan menjaga privasi individu.

**Tantangan Etika dan Hukum dalam Penggunaan Teknologi**

Meskipun teknologi canggih memberikan banyak manfaat dalam memperkuat sistem pertahanan, penggunaan teknologi tersebut juga memunculkan berbagai isu etika dan hukum (Mahendra, 2024). Salah satu isu yang paling mencolok adalah penggunaan kecerdasan buatan (AI) dalam sistem senjata otonom. Senjata otonom dapat mengambil keputusan untuk menyerang target tanpa campur tangan manusia, yang menimbulkan pertanyaan serius tentang siapa yang bertanggung jawab jika terjadi kesalahan atau kerusakan yang disebabkan oleh teknologi tersebut. Hal ini dapat menciptakan kebingungannya tentang siapa yang harus mempertanggungjawabkan tindakan yang diambil oleh mesin, terutama dalam situasi yang melibatkan korban sipil.

Selain itu, pengumpulan dan analisis data dalam skala besar yang dilakukan untuk memperkuat sistem pertahanan juga menimbulkan risiko terhadap privasi dan hak asasi manusia. Negara yang menggunakan teknologi untuk mengumpulkan informasi dapat mengakses data pribadi yang sangat sensitif, yang dapat digunakan secara tidak sah atau disalahgunakan. Dalam konteks ini, penting untuk memastikan bahwa teknologi yang digunakan tidak melanggar hak-hak individu, dan bahwa setiap pengumpulan data dilakukan sesuai dengan prinsip-prinsip dasar hak asasi manusia. Penting untuk mengembangkan kerangka hukum yang jelas dan efektif yang dapat mengatur penggunaan teknologi canggih dalam pertahanan tanpa mengabaikan prinsip-prinsip dasar hak asasi manusia. Teknologi canggih harus digunakan untuk meningkatkan keamanan, bukan untuk merusak nilai-nilai fundamental yang menjadi dasar masyarakat. Oleh karena itu, penting bagi negara-negara untuk memastikan bahwa setiap kebijakan yang melibatkan teknologi dalam pertahanan memiliki pengawasan yang tepat dan transparansi yang jelas, agar tidak terjadi penyalahgunaan.

Negara-negara merumuskan kebijakan dengan hati-hati dan transparansi dalam penggunaan teknologi dalam pertahanan. Kebijakan tersebut harus menyeimbangkan antara memperkuat kemampuan pertahanan negara dan melindungi hak asasi manusia (Sarjito, 2023). Selain itu, penting bagi negara untuk mengembangkan regulasi yang memungkinkan penggunaan teknologi dengan cara yang sah dan etis, sambil tetap menjaga keamanan nasional. Dengan pendekatan yang hati-hati, teknologi dapat dimanfaatkan secara optimal tanpa mengorbankan nilai-nilai dasar masyarakat.

Secara keseluruhan, meskipun teknologi canggih memiliki potensi besar untuk memperkuat sistem pertahanan, penggunaannya harus diawasi dan diatur dengan ketat. Negara harus mengembangkan kerangka hukum yang tidak hanya memperhatikan manfaat teknologi dalam pertahanan, tetapi juga melindungi hak asasi manusia dan privasi individu. Kebijakan yang hati-hati dan transparan sangat penting untuk memastikan bahwa teknologi digunakan dengan cara yang sah, etis, dan bertanggung jawab.



E-ISSN 2961-7553
P-ISSN 2963-8135

## KESIMPULAN

Penelitian ini menyimpulkan bahwa transformasi hukum pertahanan di era digital dan teknologi canggih menjadi kebutuhan mendesak, seiring dengan berkembangnya ancaman siber yang melintasi batas teritorial dan mempengaruhi keamanan negara. Negara-negara harus memperbarui regulasi hukum pertahanan mereka untuk mengatasi ancaman ini, terutama dalam perlindungan infrastruktur kritis dan pengaturan pertahanan berbasis teknologi. Meskipun teknologi canggih menawarkan peluang untuk memperkuat sistem pertahanan, penggunaannya juga menimbulkan tantangan terkait etika dan hukum, seperti privasi, hak asasi manusia, dan tanggung jawab hukum dalam penggunaan senjata otonom. Selain itu, globalisasi teknologi menuntut adanya pendekatan hukum yang lebih fleksibel dan kolaborasi internasional yang lebih kuat dalam menangani ancaman siber global. Oleh karena itu, negara-negara perlu segera mengembangkan kebijakan yang responsif terhadap ancaman teknologi dan memperkuat kerja sama internasional dalam bidang pertahanan dunia maya. Dengan pembaruan kebijakan yang tepat, sistem pertahanan negara dapat menghadapi ancaman di masa depan dengan lebih efektif dan responsif, serta tetap menjaga prinsip-prinsip hukum internasional dan hak asasi manusia.

## DAFTAR PUSTAKA

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *POLITIKA*, 95–110.

Aris Sarjito, & Nora Lelyana. (2023). Analisis Dampak Persepsi Ancaman Drone Terhadap Pembuatan Kebijakan Pertahanan Dan Proses Alokasi Sumber Daya. *Jurnal of Management and Social Sciences*, *1*(4), 14–32.

Berlianti, D. F., Abid, A. Al, & Ruby, A. C. (2024). Penerapan Prinsip Hukum Internasional Dalam Penegakan Hukum Terhadap Kejahatan Siber Dan Serangan Siber. *Jurnal Review Pendidikan Dan Pengajaran*, *7*(1), 1861–1864.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234.

Chatlina, C. B., Mulyana, A., & Amalia, M. (2024). Pengaruh Perkembangan Teknologi Informasi Dan Komunikasi Terhadap Kualitas Hubungan Sosial Dalam Keluarga. *KOMUNITAS: Jurnal Ilmu Sosiologi*, *7*(1), 19–38.

Chotimah, H. C. (2020). Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia. *Jurnal Diplomasi*, *7*(4), 103–123.

Duarte. (2024). Potensi dan Tantangan Inovasi dalam Manajemen Pertahanan Nasional: Membangun Keunggulan Kompetitif di Era Modern. In *Indonesia Emas Group.*

Hakim, A. N., & Yulia, L. (2024). Dampak Teknologi Digital Terhadap Pendidikan Saat Ini. *Jurnal Pendidikan Sosial Dan Humaniora*, *3*(1), 145–163.

Ichsan, M. T. (2024). Peran Telematika dalam Era Digital : Kemajuan Zaman , E-Commerce , dan Tantangan Keamanan Data. *Jurnal Telematika*, *1*(1), 1–9.



**E-ISSN 2961-7553**
**P-ISSN 2963-8135**

Irvita, M., Tribuana, R. R., & Pawari, R. R. (2025). Pembangunan Hukum di Era Digital : Tantangan dan Peluang bagi Negara dalam Menghadapi Transformasi Teknologi. *JURNAL BISNIS MAHASISWA*.

Keliat. (2024). PERAN REGULASI TERKINI DALAM MENGATASI TANTANGAN HUKUM PERBANKAN DI ERA DIGITAL. *Jurnal Darma Agung*, *32*(1), 323–331.

Kristiyanti, M., & Mahendro, I. (2025). Pemanfaatan Teknologi Informasi Dalam Membangun Strategi Keamanan Maritim di Indonesia. *Majalah Ilmiah Bahari Jogja (MIBJ)*, *23*(1), 1–10.

Kurniati, A. (2024). Study of the Artificial Intelligence Role in Achieving Cybersecurity for Critical Information Infrastructure. *MONAS: Jurnal Inovasi Aparatur*, *6*(2), 154–165.

Kusuma. (2024). Manajemen Bela Negara: Konsep dan Tata Kelola Bela Negara Menuju Indonesia Emas. In *Indonesia Emas Group.*

Mahendra. (2024). Tren Teknologi AI: Pengantar, Teori, dan Contoh Penerapan Artificial Intelligence di Berbagai Bidang. In *PT. Sonpedia Publishing Indonesia.*

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif*, *21*(3), 168.

Sarjito. (2023). Geopolitik dan Geostrategi Pertahanan: Tantangan Keamanan Global. In *Indonesia Emas Group.*

Sarjito. (2024). Kebijakan pertahanan negara dalam perspektif global. In *Indonesia Emas Group.*

Savitri, E. (2024). TRANSFORMASI DIGITAL SEBAGAI PENGUNGKIT KINERJA KEMENTERIAN PERTAHANAN. In *KEMENTERIAN PERTAHANAN*.

Syafi'i, M. H., Supriyadi, A. A., Prihanto, Y., & Gultom, R. A. G. (2023). Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia. *Journal on Education*, *5*(2), 4063–4076.



**E-ISSN 2961-7553**
**P-ISSN 2963-8135**